UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/639,948	08/17/2000	Ned Hoffman	STA-25	4850

60460 7590 11/21/2008

MARGER JOHNSON & MCCOLLOM/INDIVOS
210 SW MORRISON STREET
SUITE 400
PORTLAND, OR 97204

EXAMINER	
ZELASKIEWICZ, CHRYSTINA E	
ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
11/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/639,948	HOFFMAN, NED	
	Examiner	Art Unit	
	CHRYSTINA ZELASKIEWICZ	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16,18-24,26-48,50-56 and 58-69* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16,18-24,26-48,50-56 and 58-69* is/are rejected.

7)☒ Claim(s) *9, 12, 15, 29-31, 36-37, 41, 43-44, 47, 61-66, 69* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This action is in reply to the Amendment filed on September 11, 2008.

2. Claims 1, 4, 7, 18, 19, 23, 24, 26, 29, 32, 36, 39, 50, 51, 55, 56, 58, 64, 65 have been amended.

3. Claims 68-69 have been added.

4. Claims 17, 25, 49, 57 have been cancelled.

5. Claims 1-16, 18-24, 26-48, 50-56, 58-69 are currently pending and have been examined.

Claim Objections

6. A series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

7. A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

8. The following claims, which each depend from a dependent claim, are separated by claims that do not also depend from said dependent claim:

a. claim 69 depends upon claim 4;

b. claim 15 depends upon claim 5;

c. claim 9 depends upon claim 5;

d. claim 12 depends upon claim 10;

e. claim 64 depends upon claim 21;

f. claims 29-31 depend upon claim 26;

g. claim 66 depends upon claim 1;

h. claims 36, 37, and 61 depend upon claim 34;

i. claims 41, 43, 47 depend upon claim 37;

j. claim 44 depends upon claim 42;

k. claim 65 depends upon claim 53; and

l. claims 62-63 depend upon claim 58.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 1-16, 18-24, 26-48, 50-56, 58-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drexler (US 5,457,747), in view Gullman et al. (US 5,280,527), and further in view of Osten et al. (US 5,719,950).**

Claims 1, 32, 68

11. Drexler discloses the following limitations:

m. a user registration step, wherein a user electronically submits a registration biometric sample (biometric information) taken directly from a person of the user (C7 L30-63);

n. a public network data transmittal step, wherein the registration biometric sample (biometric information) is electronically transmitted to a master electronic identicator (library) via a public communications network (phone lines), said master electronic identicator comprising a computer database (housed in computer having extensive memory capacity) which electronically stores all of the registration biometric samples from all of the registered users (C6 L17-37, C7 L18-63);

o. a user registration biometric storage step, wherein the registration biometric sample (biometric information) is electronically stored (stored) within the master electronic identicator (library) (C7 L30-63);

p. a bid biometric transmittal step, wherein a bid biometric sample (biometric information), taken directly from the person of the user, is electronically transmitted to at least one electronic identicator (verification terminal) (C4 L35-48); and

q. a user identification step, wherein an electronic identicator (verification terminal) compares the bid biometric sample (biometric information) to at least one registration biometric sample previously stored in an electronic identicator (first writing device), for producing either a successful (matches) or failed identification of the user (C4 L35-67, C5 L1-18).

12. Drexler does not disclose the following limitations:

r. an electronic communication formation step… formed;

s. a rule-module formation step… command;

t. an electronic communication authorization step… execution;

u. a rule-module invocation step… invoked;

v. an electronic communication execution step… executed; and

w. wherein an electronic communication… cards.

13. Gullman discloses the following limitations:

x. an electronic communication formation step, wherein at least one communication (electronic funds transfer) comprising electronic data is formed (abstract);

y. a rule-module formation step, wherein a user-customized rule-module is formed in an electronic clearinghouse (host system), said rule-module further comprising at least one user-customized pattern data (PIN) associated with at least one user-customized execution command (electronic funds transfer) (abstract, C4 L3-22);

z. an electronic communication authorization step, wherein upon a successful identification (successful biometric entry) of the user by an electronic identicator, at least one electronic communication (electronic funds transfer) is authorized for execution (abstract, C4 L3-22);

aa. a rule-module invocation step, wherein upon a successful identification (successful biometric entry) of the user, at least one previously designated user-customized rule-module is invoked (abstract, C4 L3-22); and

bb. an electronic communication execution step, wherein upon the invocation of a user-customized rule- module, at least one electronic communication (electronic funds transfer) is executed (abstract, C4 L3-22).

14. Osten discloses the following limitations:

cc. wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic stripe cards (fingerprint analysis with pulse oximetry and electrocardiography) (C4 L1-14).

15. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Gullman to show 1) a user-customized rule-module is formed in an electronic clearinghouse, where said rule-module comprises at least one user-customized pattern data associated with at least one user-customized execution command; 2) a rule-module invocation step, wherein upon a successful identification of the user, at least one previously designated user-customized rule-module is invoked; and 3) an electronic communication execution step, wherein upon the invocation of a user-customized rule-module, at least one electronic communication is executed, because Gullman already teaches an electronic clearinghouse (electronic banking system) authorizing a user to perform electronic funds transfer (i.e. command) if a security token is approved (abstract, C4 L3-36). The token is based on a correlation factor (derived from biometric input) combined with a fixed code (e.g. PIN), and a time-varying code or challenge code (C4 L3-36). A suggestion exists to have 1) a user-customized rule-module, 2) a rule-module invocation step, and 3) an electronic communication execution step because said rule-module and steps can allow the user to customize his account settings (e.g. require multiple biometric parameters or change his code every 30 days) and prevent unauthorized access. Multiple biometric parameters may uniquely identify the user whereas a sole parameter may not (Osten C2 L66-67, C3 L1-28). Additionally, changing a code often (e.g. every 30 days) helps prevent unauthorized access because the code is continuously updated and harder to duplicate.

16. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures

for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claim 2

17. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

dd. during the bid biometric transmittal step, the electronic identicator comprises any of the following: a master electronic identicator, and; a subset electronic identicator (verification terminal), said subset electronic identicator comprising a computer database which electronically stores a subset of all of the registration biometric samples from registered users (C4 L35-48).

Claims 3, 35

18. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

ee. any steps of said method occur in any of the following chronological sequences: simultaneously, and; separated by any increment of time (time of day) including seconds, minutes, hours, days, weeks, months, and years (C4 L3-22).

19. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claim 4

20. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

ff. The user identification step includes a first comparison step, wherein a subset electronic identicator (verification terminal) compares the bid biometric sample (biometric information) taken directly from the person of the user (person) with at least one registration biometric sample previously stored (biometric template read from permanent storage medium) in the subset electronic identicator for producing either a successful (verified) or failed identification of the user (C 4 L 61-67, C 5 L 1); and the method further comprises:

gg. a public network data transmittal step, wherein if the subset electronic identicator returns a failed identification result (confirmed mismatch), the bid biometric sample is electronically transmitted via a public communications network (via phone lines) to a master electronic identicator (library of biometric information) (C 5 L 20-21, C 6 L 17-20, C 7 L 36-37, C 8 L 7-13);

hh. a second comparison step, wherein a master electronic identicator (library of biometric information) compares the bid biometric sample (biometric information acquired from a person at first writing device) to at least one registration biometric sample previously stored (biometric information on file at the library) in the master electronic identicator for producing either a successful or failed (does not match) identification of the user (C 6 L 20-38);

Claims 5, 37

21. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

ii. an enterprise registration step, wherein an enterprise (person) electronically submits registration identity data (biometric information) (C 7 L 31-34);

jj. a public network data transmittal step, wherein the enterprise registration identity data (biometric information) is electronically transmitted (sent via telecommunications) to a master electronic identicator (library) via a public communications network (C 7 L 35-37);

kk. an enterprise registration identity data storage step, wherein the enterprise registration identity data (biometric information) is electronically stored (store) within the master electronic identicator (library) (C 7 L 44-46);

ll. an enterprise bid identity data network transmittal step, wherein enterprise bid identity data is electronically transmitted to at least one electronic identicator, said electronic identicator comprising any of the following: a subset electronic identicator and a master electronic identicator (library) (C 7 L 35-46);

mm. an enterprise identification step, wherein an electronic identicator (library) compares the enterprise bid identity data (biometric information) with enterprise registration identity data previously stored (biometric information at the library) in the electronic identicator, for producing either a successful (yields a match) or failed identification of the enterprise (C 7 L 35-40);

nn. an electronic communication authorization step, wherein upon a successful identification of the enterprise (person) by an electronic identicator and a successful identification of the user (user) by an electronic identicator, at least one electronic communication is authorized (authorization for benefits) for execution (C 7 L 40-44, C 8 L 22-27).

22. Drexler does not disclose the following limitations:

oo. Wherein an electronic communication… swipe cards.

23. Osten discloses the following limitations:

pp. wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic swipe cards (fingerprint analysis with pulse oximetry and electrocardiography) (C4 L1-14).

24. It would have been obvious to one of ordinary skill in the art at the time of the invention to substitute “person” for “enterprise,” and “biometric information” for “registration identity data.” Drexler already teaches receiving biometric information from a person, comparing said biometric information with a biometric sample previously stored, and an authorization step based upon the successful identification of the person. Drexler does not teach receiving registration identity data from an enterprise, comparing said registration data with registration data previously stored, or an authorization step based upon the

successful identification of both the person and enterprise. However, a motivation exists to verify registration identity data from an enterprise and to use both the successful identification of the person and enterprise because two sources of identification (i.e. enterprise and person) is better than one at helping to prevent fraud and ensure proper verification, validation, and authorization (C 2 L 22-27).

25. Alternatively, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Drexler to show verifying registration identity data from an enterprise and to use both the successful identification of the person and enterprise in order to pay out benefits. Drexler already teaches verification of the person to obtain benefits from a card (abstract). These benefits may include cash, payments for goods or services, vouchers, food stamps, WIC programs, Child Immunization benefits, Medicaid, or Medicare (C 5 L 61-67). A suggestion exists to also use verification of the enterprise (i.e. specific agency that is associated with the card) because required repeated verification enhances security of the card (abstract), and ensures that the appropriate benefits (e.g. food stamps vs. Medicaid payments) are paid out to prevent fraud (C 2 L 22-27).

26. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 6, 38

27. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

qq. any steps of said method (authorization) occur in any of the following chronologies: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days (days), weeks, months, and years (C 2 L 46-50).

Claim 7

28. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

rr. The enterprise identification step includes a first comparison step, wherein a subset electronic identicator (verification terminal) compares the enterprise bid identity data (biometric information) with enterprise registration identity data previously stored (biometric template read from permanent storage medium) in the subset electronic identicator for producing either a successful (verified) or failed identification of the enterprise (C 4 L 61-67, C 5 L 1); and the method further comprises:

ss. a public network data transmittal step, wherein if the subset electronic identicator returns a failed identification result (confirmed mismatch), the enterprise bid identity data is electronically transmitted via a public communications network (via phone lines) to a master electronic identicator (library) (C 5 L 20-21, C 6 L 17-20, C 7 L 36-37, C 8 L 7-13);

tt. a second comparison step, wherein a master electronic identicator (library) compares the enterprise bid identity data (biometric information) with enterprise registration identity data previously stored (biometric information on file at the library) in the master electronic identicator for producing either a successful or failed (does not match) identification of the enterprise (person) (C 6 L 20-38);

29. It would have been obvious to one of ordinary skill in the art at the time of the invention to substitute “person” for “enterprise,” and “biometric information” for “enterprise bid identity data.” Drexler already teaches a first comparison step of biometric samples from a person with a subset electronic identicator, a second comparison step of said biometric samples with a master electronic identicator, and an authorization step based upon the successful identification of the person (claim 4 above). Drexler does not teach these first or second comparison steps for enterprise bid identity data from an enterprise, or an authorization step based upon the successful identification of both the person and enterprise. However, a motivation exists to verify enterprise bid identity data (i.e. use two comparison steps for an

enterprise) and to use both the successful identification of the person and enterprise because two sources of identification (i.e. enterprise and person) is better than one at helping to prevent fraud and ensure proper verification, validation, and authorization (C 2 L 22-27).

30. Alternatively, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Drexler to show using two comparison steps to verify enterprise bid identity data, and to use both the successful identification of the person and enterprise in order to pay out benefits. Drexler already teaches verification of the person to obtain benefits from a card (abstract). These benefits may include cash, payments for goods or services, vouchers, food stamps, WIC programs, Child Immunization benefits, Medicaid, or Medicare (C 5 L 61-67). A suggestion exists to also use verification of the enterprise (i.e. specific agency that is associated with the card) because required repeated verification enhances security of the card (abstract), and ensures that the appropriate benefits (e.g. food stamps vs. Medicaid payments) are paid out to prevent fraud (C 2 L 22-27).

Claims 8, 40

31. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

uu. the biometric sample taken directly from the person of the user comprises any of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print (voice print) (C2 L30-52).

Claims 9, 41

32. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

vv. the enterprise is a legally formed entity comprising any of the following: a corporation (bank), a foundation, a non-profit organization, a sole proprietorship, a limited liability company, and a partnership (C 4 L 32-35).

Claims 10, 42

33. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

ww. during the user identification step, the user provides a personal identification code (PIN) to the electronic identicator along with a bid biometric sample (biometric input) for purposes of identifying the user (C3 L37-55, C4 L3-22).

34. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 11, 43

35. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

xx. a user re-registration check step, wherein the user's registration biometric sample (newly acquired biometric data) is compared by at least one electronic identicator to previously registered biometric samples (biometric data previously stored) wherein if a match occurs, the electronic identicator is alerted to the fact that the user has attempted to re-register (determine if the card possessor is the same person as the registered owner) (C 2 L 53-65).

Claims 12, 44

36. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

yy. a biometric theft resolution step, wherein a user's personal identification code (authorization code number) is changed (modified) when the user's registered biometric sample is determined to have been fraudulently duplicated (C 2 L 66-67, C 3 L 1-9).

Claims 13, 45

37. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

zz. an electronic communication comprises any of the following: an email communication, a telephone call, an encrypted data packet, an Internet telephony communication (electronic funds transfer), and a facsimile (abstract, C4 L3-22).

38. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Gullman to show the electronic communication comprises an Internet telephony communication because Gullman already teaches the communication can be for an electronic funds transfer (abstract, C4 L3-22). A suggestion exists to have the communication be an Internet telephony communication because electronic funds transfer can be implemented over the Internet.

39. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 14, 46

40. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

aaa. during the communication authorization step, any of the following is used: an intranet, an extranet, a local area network, a wide area network, a cable network, a wireless network, a telephone network (phone lines), the Internet, an ATM network, or an X.25 (C7 L30-63).

Claims 15, 47

41. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

bbb. enterprise registration identity data comprises any of the following: an alpha-numeric code (authorization code number and/or alphabet sequence), a hardware identification code, an email address, a financial account, a biometric of an authorized enterprise representative, a non-financial data repository account, a telephone number, a mailing address, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, and an instant messaging address (C 2 L 66-67).

42. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Drexler to show enterprise registration identity data because Drexler already teaches a user identification code (claim 10). Therefore, a motivation exists to also utilize enterprise bid identity data because two sources of identification (i.e. enterprise and person) is better than one at helping to prevent fraud and ensure proper verification, validation, and authorization (C 2 L 22-27).

Claims 16, 48

43. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

ccc. the communication authorization step further comprises a third-party communications step, wherein the electronic identicator (security apparatus) electronically communicates with a third-party server (host system) in order to authorize the electronic communication (abstract, C4 L3-22).

44. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 18, 50, 64, 65

45. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

ddd. pattern data comprises any of the following: demographic information; an email address; a financial account (account number); internet browsing patterns; a non-financial data repository account; a telephone number; a mailing address; purchasing patterns; database authorization fields; financial credit report data; a call-center queuing, routing and automated response program; an email-center queuing, routing and automated response program; data on pre-paid accounts or memberships for products or services; electronic data utilization patterns; employee status; job title; data on user behavior patterns; a digital certificate; a network credential; an internet protocol address; a digital signature; an encryption key; an instant messaging address; user-customized medical records; an electronic audio signature; and an electronic visual signature (C4 L3-22).

46. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user

attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 19, 51

47. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

eee. said execution commands further comprise user-customized instructions for executing any of the following: accessing of stored electronic data, processing of electronic data (electronic funds transfer), and presentation of electronic data (abstract, C4 L3-36).

48. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 20, 52

49. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

fff. user-customized accessing of stored electronic data further comprises execution of any of the following: activating of an Internet-connected device; accessing of a secured physical space (secured area), and unlocking of a secured physical device (abstract, C3 L1-2).

50. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat

authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 21, 53

51. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

ggg. user-customized processing of electronic data further comprises invoking any of the following: a digital certificate, an identity scrambler, a database authorization field, an electronic consumer loyalty or consumer rewards incentive, an electronic advertisement, an instant messaging program, real-time tracking of an incoming caller or an email sender, a time and attendance monitoring program, an emergency home alarm and personal safety notification program, a real-time challenge-response program (user input challenge code), a call-center queuing prioritization program, a call-center routing prioritization program, an email-center queuing prioritization program, an email-center routing prioritization program, an automated caller or emailer response program, a call- forwarding program, and an electronic intelligent software program for electronic data search and retrieval (C2 L40-47, C3 L37-55).

52. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Gullman to show the challenge-response program is in real-time because Gullman already teaches a real time clock (C5 L1-33). A suggestion exists to have a real-time challenge-response program because this will help prevent unauthorized users from answering the challenge-response.

53. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user

attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 22, 54

54. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

hhh. user-customized presentation of electronic data comprises any of the following: a print-out, a computer screen display (monitor), an audio message (person's voice), a tactile sensation and a holographic image (C 6 L 49-67, C 7 L 1-16).

Claims 23, 55

55. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

iii. the rule-module invocation step further comprises a third-party communications step, wherein the electronic rule-module clearinghouse (security apparatus) communicates with one or more third-party computers (host systems) in order to invoke a rule-module (abstract, C4 L3-22).

56. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 24, 56

57. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

jjj. user-customized pattern data (PIN) is provided to the electronic rule-module clearinghouse (security apparatus) by any of the following: the user (user), the electronic identicator, the electronic rule-module clearinghouse, and a user-authorized third party (abstract, C4 L3-22).

58. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claims 26, 58

59. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

kkk. a master rule-module storage step, wherein all of the rule-modules from all of the registered users are stored in a master rule-module clearinghouse (host system) (abstract, C3 L19-67, C4 L1-22);

lll. a subset rule-module storage step, wherein a subset of all of the rule-modules from registered users is stored in a subset rule-module clearinghouse (security apparatus) (abstract, C3 L19-67, C4 L1-22).

60. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Gullman to show a master rule-module storage step and a subset rule-module storage step because Gullman already teaches an electronic clearinghouse authorizing a user to perform electronic funds transfer if a security token is approved (abstract, C4 L3-36). The token is based on a correlation factor (derived from biometric input) combined with a fixed code (e.g. PIN), and a time-varying code or challenge code (C4 L3-36). A suggestion exists to have a master rule-module storage step and a subset

rule-module storage step because said rule-modules can allow the user to customize his account settings (e.g. require multiple biometric parameters or change his code every 30 days) and prevent unauthorized access. For example, multiple biometric parameters (e.g. voice and facial scan) may uniquely identify the user whereas a sole parameter (e.g. voice) may not. Changing a code every 30 days also helps prevent unauthorized access because the code is continuously updated.

61. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claim 27

62. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

mmm. during the registration biometric network transmittal step, any of the following public networks is used: a cable network, a wireless cellular network, a wireless digital network, a telephone network (phone lines), a wide area network, the Internet, an ATM network, and an X.25 connection (C7 L30-63).

Claims 28, 59

63. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

nnn. during the public network data transmittal step, any of the following networks is used: a cable network, a wireless cellular network, a wireless digital network, a telephone network (phone lines), a wide area network, the Internet, an ATM network, and an X.25 connection (C7 L30-63).

Claim 29

64. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

ooo. The rule-module invocation step includes a first rule-module invocation step, wherein the subset rule-module clearinghouse (security apparatus) attempts to invoke at least one user-customized rule-module (proper PIN) (abstract, C3 L19-67, C4 L1-22); and the method further comprises:

ppp. a public network data transmittal step, wherein if the subset rule-module clearinghouse (security apparatus) fails to invoke a user-customized rule-module, the request is transmitted to a master rule-module clearinghouse (host system) via a public communications network (abstract, C3 L19-67, C4 L1-22);

qqq. a second rule-module invocation step, wherein a master rule-module clearinghouse (host system) attempts to invoke at least one user-customized rule-module (abstract, C3 L19-67, C4 L1-22).

65. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Gullman to show if the subset rule-module clearinghouse fails to invoke a user-customized rule-module, the request is transmitted to a master rule-module clearinghouse via a public communications network, because Gullman already teaches the security apparatus sending the token output directly to the host system (abstract, C3 L19-67, C4 L1-22). A suggestion exists to have the subset clearinghouse (security apparatus) transmit the token output to the master clearinghouse (host system) because the host can verify the identification, and permit full or limited entry based on the level of authorization assigned.

66. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user

attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claim 30

67. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

rrr. the master rule-module clearinghouse (host system) comprises a computer database (database) which electronically stores all of the rule-modules (PINs) for all of the registered users (abstract, C3 L19-67, C4 L1-22).

68. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claim 31

69. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

sss. the subset rule-module clearinghouse (security apparatus) comprising a computer database which electronically stores a subset of all of the rule-modules (PINs) for registered users (figure 2, C3 L19-67, C4 L1-22).

70. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat

authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claim 33

71. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

ttt. the master electronic identicator (library) further comprises a computer database which: has a location which is physically remote from the site at which the user submits a biometric sample directly from his person, and; requires the use of a public communication network (phone lines) that enables receipt of an electronically transmitted registration biometric sample (figures 1-2, C6 L17-37, C7 L18-63).

Claim 34

72. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

uuu. a subset electronic identicator (verification terminal) having:

vvv. a computer database containing a subset of all stored biometric samples from registered users in the computer system (see claim 31 above);

www. a comparator that compares a received biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user (see claim 4 above).

Claims 36, 39

73. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

xxx. a data transmittal public network, comprising a public communications network (phone lines) that electronically transmits data between the subset electronic identicator (verification

terminal) and a master electronic identicator (library) if the comparator of the subset electronic identicator returns a failed identification result (C 4 L 61-67, C 5 L 1).

74. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Drexler to show transmitting the data to the master identicator if the comparator of the subset electronic identicator returns a failed identification result because the library can determine whether or not there is a match with biometric information under a different name, social security number or other common identification (C7 L30-63).

Claim 60

75. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

yyy. the master electronic identicator (library) further comprises a computer database having a location which is physically remote from the site at which the user submitted the registration biometric sample (figures 1-2, C6 L17-37, C7 L18-63).

Claim 61

76. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

zzz. the subset electronic identicator (verification terminal) further comprises a computer database (see claim 31 above):

aaaa. being physically remote from the master identicator (figure 1, C 6 L 18-23, C 8 L 22-27);

bbbb. capable of using any communications network (computer) for receiving the bid biometric sample (biometric information) (C 6 L 49-67).

Claim 62

77. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Gullman discloses the following limitations:

cccc. a first rule-module invocation platform, comprising a subset rule-module clearinghouse that invokes at least one user-customized rule-module (see claim 29);

dddd. a data transmittal public network, wherein if the subset rule-module clearinghouse fails to invoke a user-customized rule-module, the request is transmitted via a public communications network to a master rule-module clearinghouse (see claim 29);

eeee. a second rule-module invocation platform, comprising a master rule-module clearinghouse that invokes at least one user-customized rule-module (see claim 29);

ffff. an electronic communication execution platform, that executes at least one electronic communication (electronic funds transfer) upon the earliest invocation of a user-customized rule-module by a rule- module clearinghouse (abstract, C3 L19-67, C4 L1-22).

78. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Drexler, in view of Gullman, and further in view of Osten because 1) a need exists to deter fraud in electronic benefit transfer systems (Drexler C 2 L 22-27); 2) a need exists to provide security measures for safeguarding access to information (Gullman C1 L1-67, C2 L1-17); and 3) a need exists to combat authentication systems that would erroneously accept authentication of a truly unauthorized user attempting to gain access using the pattern of a unique, inherently specific biometric parameter from an authorized user (Osten C2 L35-45).

Claim 63

79. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

gggg. the subset rule-module clearinghouse (verification terminal) is physically remote from the master rule-module clearinghouse (library) (figure 1, C 6 L 18-23, C 8 L 22-27).

Claims 66, 67

80. See rejection above for claims 1 and 10.

Claim 69

81. Drexler, in view of Gullman and Osten, discloses the limitations above. Furthermore, Drexler discloses the following limitations:

hhhh. second user registration biometric storage step, wherein the registration biometric sample (biometric information) is electronically stored within the subset electronic identicator (verification terminal) (C4 L35-48).

82. **Examiner's Note**: The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Double Patenting

83. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

84. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

85. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

86. The instant application is provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over copending application 11/321,114 and US patent 6,012,039. Although the conflicting claims are not identical, they are not patentably distinct from each other because the subject matter of the instant application would have been obvious to one of ordinary skill in the art in light of the disclosure of applications 11/321,114 and US patent 6,012,039. The instant application is directed to comparing biometric samples taken from a user to biometric samples stored in an electronic identicator; and upon successful identification, invoking a rule-module. Application 11/321,114 is directed to successfully identifying biometric samples and at least one rule module. US patent 6,012,039 is directed to comparing biometric samples from an issuer with samples stored at an electronic identicator, and upon successful identification, a reward transaction is authorized. The instant application would have been obvious to one of ordinary skill in the art in light of application 11/321,114 and US patent 6,012,039 because both encompass identification based on biometric samples, and upon successful identification, authorizing an action (analogous to invoking a rule-module).

87. This is a provisional obviousness-type double patenting rejection regarding application 11/321,114 because the conflicting claims have not in fact been patented.

Response to Arguments

88. Applicant's arguments are moot in light of the new art applied above.

Conclusion

89. Applicant's amendment filed on September 11, 2008 necessitated the new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 C.F.R. §1.136(a).

90. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 C.F.R. §1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

91. Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **Chrystina Zelaskiewicz** whose telephone number is **571.270.3940.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, **Andrew Fischer** can be reached at **571.272.6779**.

92. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

/Chrystina Zelaskiewicz/
Examiner, Art Unit 3621
November 18, 2008

/ANDREW J. FISCHER/
Supervisory Patent Examiner, Art Unit 3621